IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

SECURITIES AND EXCHANGE COMMISSION, Plaintiff, v. SOLARWINDS CORP. and TIMOTHY G. BROWN, Defendants.	)	Civil Action No. 1:23-cv-09518-PAE-BCM

DECLARATION OF DANIELLE CAMPBELL IN SUPPORT OF DEFENDANTS' MOTION FOR SUMMARY JUDGMENT

I, Danielle Campbell, hereby declare under penalty of perjury, pursuant to 28 U.S.C. § 1746, as follows:

1. I am the Senior Director of Internal Audit at SolarWinds (the "Company"), a position I have held since February 2020. Prior to that, I held the position of Director of Internal Audit at SolarWinds from 2011 to 2020. I was in charge of SolarWinds' internal audit program throughout the Relevant Period in this case (October 2018 to January 2021). I make this declaration in support of SolarWinds' and Tim Brown's motion for summary judgment. The facts set forth herein are based on my personal knowledge and my review of SolarWinds records. If called upon to do so, I can and will competently testify to these facts.

2. I understand that the Securities and Exchange Commission (SEC) relies on certain excerpts of documents related to Sarbanes-Oxley (SOX) audits of the Company during the Relevant Period to argue that the Security Statement's representations concerning role-based access controls and passwords were false. I submit this declaration to explain these documents and to clarify that they do not contradict the representations in the Security Statement.

3. **March 2020 Email Re: Control Deficiencies.** First, I understand the SEC relies on a March 2020 email I sent to a group of SolarWinds managers, letting them know that their teams' assistance would be needed to remediate certain "control deficiencies" identified in the SOX audit of the Company for Fiscal Year (FY) 2019. *See* Ex. A (SW-SEC00388330). The email attaches a spreadsheet, which I prepared, reflecting the control deficiencies found in the audit and their remediation status. *See* Ex. B (SW-SEC00388332). The FY 2019 SOX audit did not find, and nothing in the email or spreadsheet suggests, that there was any significant failure to implement role-based access controls or password requirements as described in the Security Statement.

4. As an initial matter, the deficiencies reflected in the spreadsheet were merely control deficiencies. Under the auditing standards applicable to SOX, which I am familiar with in my role as Senior Director of Internal Audit, there are three types of deficiencies: control deficiencies, significant deficiencies, and material weaknesses. Control deficiencies are minor and not considered to pose any significant risk to the accuracy of a company's financial statements (the focus of SOX audits). A *significant* deficiency, by contrast, creates a risk that a "more than inconsequential" error in a company's financial statements will go unprevented or undetected. A *material weakness* is a deficiency that creates a risk that a *material* error in a company's financial statements will go unprevented or undetected. SEC rules only require disclosure of material weaknesses in their public filings. And auditors are only required to report material weaknesses and significant deficiencies to management. Reporting mere control deficiencies to management is done simply as good practice.

5. The fact that none of the deficiencies found in the Company's IT General Controls in the FY 2019 SOX audit were significant deficiencies or material weaknesses can be seen in

Column J of the "IT Deficiencies" tab for these controls—labeled "Exception Type (MW, SD, CD)," *i.e.*, "material weakness," "significant deficiency," or "control deficiency." All of the entries in the column are labeled "CD." Ex. B.

6. The spreadsheet also includes an explanation for why each control deficiency was considered to be minor. This is found in Column M, labeled "Why the impact is not pervasive?" *See* Ex. B.

7. Further, while some of the deficiencies concern issues relating in some way to access controls or passwords, that does not mean they relate to any representations made in the Security Statement about access controls or passwords.

a. For example, one password-related control deficiency was that, on one system examined, password complexity was enforced, but password age and history requirements were not (*i.e.*, requirements that, after a certain number of days, passwords be changed to a password not previously used by the user).[1] *See* Ex. B ("IT Deficiencies" tab at Row 7). The Security Statement, however, says nothing about the Company's password age and history requirements.

b. As another example, one control deficiency concerned the fact that, for one of the systems examined, a user access review was prepared by an employee with privileged access to the system, in which case SOX auditing protocols require that an independent reviewer must review that employee's access, which had not been done in this case. *See* Ex. B ("IT Deficiencies" tab at Row 9). This is a technical auditing issue that has nothing to do with whether role-based access controls were in place.

[1] This deficiency was found to be minor because users generally had to log into the Company's corporate network in order to access the system, and password age and history requirements were enforced on the network login.

8. While some of the deficiencies on the spreadsheet concern oversights in the access-provisioning process, the details provided in the spreadsheet make clear they were limited in scope. For example, for one system examined, there were only two users out of a sample of 30 for whom the auditors could not find sufficient evidence of approval for their access prior to provisioning. *See* Ex. B ("IT Deficiencies" tab at Row 11). Moreover, while no evidence of prior approval could be found for these two users, the access they received was appropriate for the user to obtain based on their role.

9. None of the deficiencies covered in the spreadsheet concern any pervasive problem with the Company's role-based access controls or password controls. That is why there is an explanation in the spreadsheet for each of the deficiencies concerning "[w]hy the impact is not pervasive." *See* Ex. B ("IT Deficiencies" tab at Column M). If there had been a finding that the Company was pervasively failing to implement role-based access controls or password controls on financially significant systems, that would have been identified as a material weakness, not a mere control deficiency. I note that in my email about the control deficiencies found in the audit, I stated that "for our first year as a public company, I believe the teams did a good job." Ex. A at -331. While I flagged that there were "areas for improvement" identified in the audit, that is to be expected in any audit.

10. **Slide Concerning Problems Encountered in Preparing for 2020 SOX Audit.** I understand the SEC also relies on a slide in a Quarterly Risk Review (QRR) presentation from May 2020 labeled "Q1 2020 AD Access Audit Deficiency | Remediation." Ex. C (SW-SEC00148267) at -283. This slide was not prepared by me, but I am familiar with the issue it was about. It was not actually about a deficiency finding in our FY 2020 SOX audit. It was about a couple of issues that we encountered during our SOX *planning review* that we conducted with our

internal and external auditors. (The slide was prepared by someone outside Internal Audit, in the IT organization, who was using audit language in the slide imprecisely.)

11. Specifically, in completing a user access review of Active Directory (the gateway to SolarWinds' corporate network) for Q1 2020, we discovered two issues: (1) the list of vendors and contractors the Company was checking Active Directory user accounts against (to see if the accounts belonged to active users) was incomplete; and (2) employees who were active in the previous quarter (Q4 2019) but terminated in Q1 2020 were still listed as active in Active Directory. After these issues were identified, the Company promptly fixed the underlying problems before Q2 2020 so that the user access review could be accurately conducted. These issues did not ultimately result in any control deficiency being found as part of our outside auditor's FY 2020 SOX audit findings.

12. Nothing in this slide concerns any pervasive failure to implement role-based access controls as described in the Security Statement. Rather, the slide concerned one-time problems we encountered in our processes for conducting user access reviews for SOX audits. I note that user access reviews are not even mentioned in the Security Statement.

13. **Slide from May 2019 Slide Deck Regarding SOX Compliance Preparations.** Finally, I understand the SEC has cited, within a May 2019 slide deck about security and compliance initiatives, a slide titled "Financial: Enterprise Access Management (SOX Compliance)." Ex. D (SW-SEC00001635) at -644. The slide is about an ongoing project for which I am listed as the "Lead." This slide related to our efforts to prepare for our first SOX audit after our 2018 initial public offering, by ensuring that we had documentation and processes related to access management that were aligned with SOX requirements. As is evident from the "Key

Milestones / Status" section on the right side of the slide, most of the work for the project had been completed by early 2019. The only part of the project still ongoing was the SOX audit itself.

14. I understand that the SEC has pointed to the notations on the left hand of the slide, under "Issues, Risks & Dependencies," stating "Concept of least privilege not followed as a best practice" and "Use of shared accounts throughout internal and external applications." Ex. D at -644. This text appears to have been copied over from a progress slide for an earlier project led by Eric Quitugua that was started in 2017, which involved auditing user accounts to validate their privilege levels and access permissions. *See* Ex. E (SW-SEC00042893) at -907. It appears from that slide that part of the earlier project involved ensuring that access controls and permissions were aligned with applicable security standards and guidelines, work that was in progress in early 2018. As the Company began preparing for its IPO in 2018, this work may have morphed into a broader project to review our access management processes against SOX requirements. I believe that is what is meant in the notation on the left half of the later slide that says "Project scope expanded to include SOX compliance requirements."

15. I do not know what the notations "Concept of least privilege not followed as a best practice" and "Use of shared accounts throughout internal and external applications" were originally intended to refer to. But I am certain that they do *not* refer to any pervasive problem implementing the concept of least privilege or preventing the use of shared accounts that was uncovered as part of our SOX-related work. No such deficiency was ever found in any SOX audits or preparations for SOX audits during the Relevant Period.

[*signature on following page*]

I declare under penalty of perjury that the foregoing is true and correct.

Executed on: April 24, 2025

Danielle Campbell